REMARKS/ARGUMENTS

Claims 1, 3, 5, 7, 8, 10-12, 19, 20, 22-24, 28-32, 34, 38-41, 48-50, 72, 73, 75-81, and 93 are pending in the application. Claims 1, 3, 5, 7, 8, 10-12, 19, 20, 22-24, 28-32, 34, 38-41, 48-50, 72, 73, 75-81, and 93 stand rejected as obvious under 35 U.S.C. § 103. The rejection is respectfully traversed and reconsideration is requested. The references asserted do not teach or suggest the claimed invention.

Claim Rejections - 35 U.S.C. § 103

Claims 1, 3, 5, 7, 8, 10-12, 19, 20, 22-24, 28-32, 34, 38-41, 48-50, 72, 73, 75-81, and 93 stand rejected under 35 U.S.C. § 103(a) as obvious over Fischer, Rosen, Public Legal Education of Nova Scotia, and Shannon.

In paper 6, the Examiner considered that Fischer teaches every element of independent claims 1 and 81 except escrowing the secret device being conditioned on the occurrence of an event (other than loss of a password), which the Examiner considered to be taught by Legal Education of Nova Scotia and Rosen. However, the Examiner considered that claims 13, 37-40, 43, 57-61, 63-66, and 68-71 depending on independent claim 1 were allowable, because Fischer, Rosen and/or Legal Education of Nova Scotia do not teach or suggest a virtual executor function of an electronic wallet application. In the Response filed July 26, 2001, claims 32, 41, 56, 62, and 67 were rewritten in allowable independent form as suggested by the Examiner, and in addition, independent claims 1 and 81 were amended, e.g., to include a similar limitation.

In paper 9, based on a conversation with his Supervisor, the Examiner reversed his position on the allowability of claims 13, 37-40, 43, 57-61, 63-66, and 68-71 and considered that Fisher and Rosen teach all the limitations of the amended claims because the virtual executor function of the virtual wallet application is not patentably significant in that it is simply a label for unpatentable steps and that there is nothing in the claim language that indicates that the steps are carried out by the virtual executor. In the Response filed on December 28, 2001, independent claims 56, 62, and 67 were

canceled, and independent claims 1, 32, 41, and 81were further amended to add limitations proposing, e.g., that the virtual wallet functionality is programmed to escrow a secondary aspect of a secret access device for accessing data stored on the virtual wallet application conditioned on the occurrence of an event, such as death or incompetence, that renders the owner incapable of acting on the owner's own behalf, and upon receiving verification of the occurrence of the event, to provide access to the stored data utilizing the secondary aspect of the secret access device.

In paper 12, the Examiner nevertheless considered that Fischer in view of Rosen teaches every element of amended independent claims 1, 32, 41, and 81 and all the claims depending on them. In the Preliminary Amendment filed with a Request for Continued Examination on September 18, 2002, new claim 93 was added with a further limitation proposing, e.g., that the secondary aspect of the secret access device is escrowed by the virtual executor function to allow access to the owner's stored data only to an authorized representative of the owner's estate, that the owner is allowed to store data relating to the owner's estate on the local aspect, and that the remote aspect is periodically updated with the data stored on the local aspect by a virtual archivist function of the virtual wallet application.

In paper 16, the Examiner allowed claim 93, because Fischer, Rosen, and Legal Education of Nova Scotia do not teach or render obvious the method for securely storing data for an owner according to the combined steps of claim 93, and in particular, that Legal Education of Nova Scotia fails to anticipate or render obvious the step within the escrowing process of the remote aspect being periodically updated with data stored on the local aspect by a virtual archivist function of the virtual wallet application. In the Response filed April 22, 2003, independent claims 1, 32, 41, and 81 were further amended to include, e.g., a limitation similar to allowed claim 93 of the step within the escrowing process of the remote aspect being periodically updated with data stored on the local aspect by a virtual archivist function of the virtual wallet application.

In paper 19, the Examiner again reversed his position on allowance and considered that Fischer, Rosen, Legal Education of Nova Scotia, and Shannon disclose all the elements of independent claims 1, 32, 41, 81, and 93 and all of the claims depending on them.

As presently constituted, independent method claims 1, 32, 41, and 93, and independent system claim 81 propose, e.g., that data consisting at least partly of information relating to the owner's estate is stored for the owner by entering the data on a virtual wallet application that has a local aspect residing on a terminal of the owner, a remote aspect residing on a trusted third party's server coupled to the terminal via a network, and that also has a virtual executor function. The virtual wallet application automatically assigns a primary aspect of a secret device for accessing the stored data to the owner, and the virtual executor function of the virtual wallet application automatically escrows a secondary aspect of the secret access device conditioned on the occurrence of an event that renders the owner incapable of acting on his own behalf. The remote aspect of the virtual wallet application is periodically updated with the data stored on the local aspect by a virtual archivist function of the virtual wallet application via the network, and upon receipt of verification of the occurrence of the event from the owner's personal representative by the trusted third party, the escrowed secret access device is used by the trusted third party to access the stored data on behalf of the owner's personal representative.

It is respectfully submitted that Fischer, Rosen, Legal Education of Nova Scotia, and/or Shannon do not disclose or suggest Applicants' claimed invention either separately or in combination with one another. The Examiner considers that Fischer teaches storing data for the owner, assigning a secret password to access the stored data, automatically escrowing the information, and receiving verification from the owner to access the stored data. According to Fischer, in order to protect against forgetting a password under which a PC purchaser stores data on his PC, the purchaser also stores information uniquely identifying himself together with his password on his PC under the public key of the PC seller or maker as an escrow security record. Thereafter, if

the purchaser forgets his password, he can present evidence to the PC seller or maker for comparison to the identification information stored under the seller's or maker's public key to verify his identify, whereupon the PC seller or maker reveals its private key to the purchaser to access his password previously stored under the public key. See, e.g., Col. 2, line 19-Col. 3, line 52.

It is true that Fischer discloses storing data for the owner under his password, but there is absolutely no suggestion in Fischer of storing data consisting at least partly of information relating to the owner's estate on a virtual wallet application that has a local aspect residing on the owner's terminal and a remote aspect residing on a trusted third party's server coupled over a network to the terminal, and which also has a virtual executor function, according to Applicants' claimed invention. It is likewise true that Fischer discloses storing the PC owner's password separately, but there is no suggestion whatsoever in Fischer of automatically assigning a primary aspect of a secret access device for the virtual wallet application to the owner by the virtual wallet application for accessing the stored data and automatically escrowing a secondary aspect of the secret access device for the virtual wallet application by the virtual executor function conditioned on the occurrence of an event that renders the owner incapable of acting on the owner's own behalf, according to Applicants' claimed invention. Rather, Fischer focuses on allowing the purchaser of the PC to protect himself against forgetting his password by entering unique identifying information together with his password on his PC and storing both under the public key of the PC seller or maker (which is therefore inaccessible to the PC owner without the private key from the maker or seller).

(1)

(2)

It is also true that Fischer discloses accessing the stored information upon verification by the PC purchaser of his identity to the PC maker or seller. However, there is nothing at all in Fischer to suggest verifying the occurrence of an event that renders the owner incapable of acting on his own behalf to the trusted third party by the owner's personal representative and accessing the stored data by the trusted third party on behalf of the owner's personal representative with the escrowed secret access device, according to Applicants' claimed invention. On the contrary, according to

(3)

Fischer, if the PC owner forgets the password that he stored on his PC with his identifying information under the public key of the PC maker or seller, he can verify his identity to the PC maker or seller by presenting evidence of the identifying information to the PC maker or seller for comparison to the identifying information that he actually stored, and if satisfied by the comparison, the maker or seller can disclose its private key to the PC owner with which the owner can access the password stored under the maker's or seller's public key.

Rosen does not remedy the deficiencies of Fischer. The Examiner considers that Rosen illustrates an example of automation or 'electronification' of the banking industry. According to Rosen, subscribers are provided with computer modules for storing electronic money issued by banks, and the modules can be embedded in hand-held computers that can be carried around like wallets. The computer modules can be used by subscribers to perform transactions with on-line systems of participating banks or to exchange the electronic money with other subscribers in off-line transactions. Participating banks are also provided with computer modules with which they can interface to subscribers' computer modules to perform on-line transactions. See, e.g., Col. 3, line 40-Col. 5, line 44.

It is true that Rosen discloses an electronic monetary system. However, there is absolutely nothing in Rosen to suggest storing data relating to the owner's estate on a virtual wallet application with a local aspect that resides on the owner's terminal and a remote aspect that resides on a trusted third party's server coupled to the terminal via a network, and which also has a virtual executor function, assigning a primary aspect of a secret access device for the virtual wallet application to the owner by the virtual wallet application, escrowing a secondary aspect of the secret access device by the virtual executor function conditioned on the occurrence of an event that renders the owner incapable of acting on his own behalf, and upon receiving verification of the occurrence of the event by the trusted third party from a personal representative of the owner, accessing the stored data by the trusted third party on behalf of the owner's personal representative with the escrowed secret access device, according to

Applicants' claimed invention. Rather, Rosen focuses on providing subscribers with computer modules for storing electronic money issued by banks, and which can be embedded in hand-held computers that can be carried around like physical wallets that can be used by the subscribers in transactions with on-line systems of participating banks or to exchange electronic money with one another in off-line transactions, and likewise providing participating banks with computer modules they can use to interface to subscribers' computer modules to perform on-line transactions.

Nor does Legal Education of Nova Scotia cure the deficiencies of Fischer and/or Rosen. The Examiner considers that Legal Education of Nova Scotia teaches that banks rent safe deposit boxes in which renters can store documents which are held in escrow conditioned on an event such as the death of the renter. It is true that banks rent safe deposit boxes in which the renters can store documents and to which they are given keys for access. It is also true that Banks do not allow access to the contents of a box after the death of its renter except for the limited purpose of searching for a will or burial plot deed However, there is absolutely no suggestion in Legal Education of Nova Scotia of storing data relating to the owner's estate on a virtual wallet application with a local aspect that resides on the owner's terminal and a remote aspect that resides on a trusted third party's server coupled to the terminal via a network, and which also has a virtual executor function, assigning a primary aspect of a secret access device for the virtual wallet application to the owner by the virtual wallet application, escrowing a secondary aspect of the secret access device by the virtual executor function conditioned on the occurrence of an event that renders the owner incapable of acting on his own behalf, and upon receiving verification of the occurrence of the event by the trusted third party from a personal representative of the owner, accessing the stored data by the trusted third party on behalf of the owner's personal representative with the escrowed secret access device, according to Applicants' claimed invention. On the contrary, there is patently no escrow of the contents of the safe deposit box for the renter of the box by the bank subject to fulfillment of a condition. Rather, in order to prevent inheritance tax fraud, tax laws

make it a crime for banks to allow access to the contents of the box after the death of the renter until the tax authorities complete their own inventory of the box with the limited exception of searching in the presence of a bank employee for the will or burial plot deed on presentation of a death certificate by the decedent's next-of-kin. Otherwise, there is absolutely nothing to stop the renter or anyone else with a key to the box from accessing its contents at any time during the lifetime of the renter. Likewise, after the tax authorities complete their inventory, there is absolutely nothing to stop anyone with a key to the box from accessing its contents after the renter's death.

Nor does Shannon remedy the deficiencies of Fischer and/or Rosen and/or Legal Education of Nova Scotia. The Examiner considers that Shannon discloses an archiving system with a local aspect on a terminal and a remote aspect on a server coupled to the terminal via a network and periodically updating the remote aspect with data stored on the local aspect. According to Shannon, a PC user backs up his PC hard disk by creating and saving a data file reflecting a complete logical disk map of his PC hard disk and storing a copy on a back-up server. The PC periodically updates the disk map and compares it to the existing disk map, creates a list of modified and removed files, sends the modified files to the back-up server and deletes the removed files from the back-up server. See, e.g., Col. 2, line 56-Col. 3, line 35.

While it is true that Shannon teaches a system for backing up and updating a disk map of a PC hard disk a back-up server, there is absolutely no suggestion in Shannon of storing estate data for the owner on a virtual wallet application with a local aspect residing on the owner's terminal and a remote aspect residing on a trusted third party's server, and which also has a virtual archivist function that periodically updates the remote aspect of the virtual wallet application with the data stored on the local aspect, according to Applicants' claimed invention. On the contrary, according to Shannon, the PC user backs up his PC hard disk by creating and saving a logical disk map of his hard disk, storing a copy of the disk map on the back-up server, periodically updating the disk map and comparing it to the existing disk map, and

creating a list of modified and removed files and sending the modified files to the back-up server and deleting the removed files from the back-up server.

Accordingly, Fischer and/or Rosen and/or Legal Education of Nova Scotia and/or Shannon, either separately or in combination with one another, do not disclose, or even suggest, the required combination of limitations of independent claims 1, 32, 41, 81, and 93 of Applicant's claimed method and system for securely storing data for an owner. On the contrary, it is believed that the Examiner inadvertently allowed improper hindsight to intrude into the analysis by reading the Applicants' own teachings into the prior art.

Because the cited references, either alone or in combination, do not teach the limitations of independent claims 1, 32, 41, 81, and 93, the Examiner has failed to establish the required prima facie case of unpatentability. See In re Royka, 490 F.2d 981, 985 (C.C.P.A., 1974) (holding that a prima facie case of obviousness requires the references to teach all of the limitations of the rejected claim); See also MPEP §2143.03. The Examiner has failed to establish the required prima facie case of unpatentability for independent claims 1, 32, 41, 81, and 93, and similarly has failed to establish a prima facie case of unpatentability for claims 3, 5, 7, 8, 10-12, 19, 20, 22-24, 28-31, 48-50, 72, 73, and 75-80 that depend on claim 1 and claims 34 and 38-40 that depend on claim 32, and which recite further specific elements that have no reasonable correspondence with the references.

Conclusion

In view of the foregoing amendment and these remarks, each of the claims remaining in the application is in condition for immediate allowance. Accordingly, the examiner is requested to reconsider and withdraw the rejection and to pass the application to issue. The examiner is respectfully invited to telephone the undersigned at (336) 607-7318 to discuss any questions relating to the application.

Respectfully submitted,

Date: 12/19/03

John M. Harrington (Reg. No. 25,592)
for George T. Marcou (Reg. No. 33,014)

Kilpatrick Stockton LLP
607 14th Street, NW, Suite 900
Washington, DC 20005
(202) 508-5800

T0091-178714
WINLIB01:1045660.1